ON THE CONGRUENCE $x^{\phi(P)} \equiv 1$, MOD. P^n.

BY PROFESSOR JACOB WESTLUND.

(Read before the American Mathematical Society, August 31, 1903.)

1. Let $k(\theta)$ be any algebraic number field and P a prime ideal in $k(\theta)$. Then we know that every algebraic integer, which is prime to P, satisfies the congruence

$$x^{\phi(P)} \equiv 1, \text{ mod. } P, \tag{1}$$

where $\phi(P) = n(P) - 1$, $n(P)$ denoting the norm of P. The object of the present note is to determine the roots of the congruence

$$x^{\phi(P)} \equiv 1, \text{ mod. } P^n, \tag{2}$$

for $n > 1$.*

2. To determine the roots of (2) we introduce the function $q_n(\alpha)$, defined in the following way. Suppose that α be a root of

$$x^{\phi(P)} \equiv 1, \text{ mod. } P^n,$$

and let μ_n be an algebraic integer, divisible by P^n and by no higher power of P. Then we can find an algebraic integer, which we denote by $q_n(\alpha)$, such that

$$\alpha^{\phi(P)} \equiv 1 + \mu_n q_n(\alpha), \text{ mod. } P^{n+1}. \tag{3}$$

For if

$$\alpha^{\phi(P)} = 1 + \pi,$$

where π is divisible by P^n, we should have

$$\pi \equiv \mu_n q_n(\alpha), \text{ mod. } P^{n+1},$$

and

$$\frac{\gamma\pi}{\mu_n} \equiv \gamma q_n(\alpha), \text{ mod. } P, \tag{4}$$

if γ is an algebraic integer, prime to P, such that $\gamma\pi/\mu_n$ is an

* For $k(1)$ or the number field consisting of the rational numbers, see Bachmann: Niedere Zahlentheorie, p. 159.

integer. Since γ is prime to P, the congruence (4) determines $q_n(\alpha)$ uniquely mod. P. The function q_n, defined in this way, depends on μ_n. But if μ_n and μ_n' be two algebraic integers, divisible by P^n and by no higher power of P, and q_n and q_n' the corresponding functions q, then

$$(5) \qquad \mu_n q_n(\alpha) \equiv \mu_n' q_n'(\alpha), \text{ mod. } P^{n+1}.$$

3. For the function $q_n(\alpha)$ we can easily derive the following three properties:

I. $q_n(\alpha\beta) \equiv q_n(\alpha) + q_n(\beta)$, mod. P.

II. $q_n(\alpha) \equiv q_n(\beta)$, mod. P, if $\alpha \equiv \beta$, mod. P^{n+1}.

III. $q_n(\alpha) \equiv q_n(\beta) - \beta'\delta'\pi\delta/\mu_n$, mod. P, if $\alpha \equiv \beta$, mod. P^n.

Here $\pi = \alpha - \beta$ and δ is an algebraic integer, prime to P, such that $\pi\delta/\mu_n$ is an integer. β' and δ' are determined by $\beta\beta' \equiv 1$, mod. P, and $\delta\delta' \equiv 1$, mod. P.

The first two properties follow directly from the definition of $q_n(\alpha)$. To prove the third property let $\alpha = \beta + \pi$. Then, since $\phi(P) = p^f - 1$, p being the rational prime divisible by P and f the degree of P, we have

$$\begin{aligned}(\beta + \pi)^{\phi(P)} &\equiv \beta^{\phi(P)} - \beta^{\phi(P)-1}\pi, \text{ mod. } P^{n+1}, \\ &\equiv \beta^{\phi(P)} - \beta'\beta^{\phi(P)}\pi, \text{ mod. } P^{n+1}, \\ &\equiv 1 + \mu_n q_n(\beta) - \beta'\pi, \text{ mod. } P^{n+1},\end{aligned}$$

and hence

$$\mu_n q_n(\alpha) \equiv \mu_n q_n(\beta) - \beta'\pi, \text{ mod. } P^{n+1},$$

from which the third property follows directly.

4. Now let α be a root of

$$(6) \qquad x^{\phi(P)} \equiv 1, \text{ mod. } P^n.$$

Let β be any algebraic integer and P^m the highest power of P, which will divide $\beta - \alpha$. Then, if we set $\beta = \alpha + \pi$, in order that β should be a root of

$$(7) \qquad x^{\phi(P)} \equiv 1, \text{ mod. } P^{n+1}$$

we must have

$$(\alpha + \pi)^{\phi(P)} \equiv 1, \text{ mod. } P^{n+1},$$

or

$$(8) \qquad \mu_n q_n(\alpha) + \phi(P)\alpha'\pi + \frac{\phi(P)[\phi(P) - 1]}{2\,!}\alpha'^2\pi^2$$

$$+ \cdots + \alpha'^{\phi(P)} \pi^{\phi(P)} \equiv 0, \text{ mod. } P^{n+1},$$

where $\alpha\alpha' \equiv 1$, mod. P^n.

If $m < n$, all the terms in (8) would be divisible by P^m, and hence $\phi(P)$ divisible by P, which is impossible. Hence we must have $m = n$. Then we get from (8)

$$\pi \equiv \alpha\mu_n q_n(\alpha), \text{ mod. } P^{n+1},$$

and

$$(9) \qquad \beta \equiv \alpha[1 + \mu_n q_n(\alpha)], \text{ mod. } P^{n+1}.$$

It is also easily seen that $\alpha[1 + \mu_n q_n(\alpha)]$ is a root of (7), if α is a root of (6). Now let α_1 and α_2 be two roots of (6), incongruent mod. P^n. Then, if

$$\alpha_1[1 + \mu_n q_n(\alpha_1)] \equiv \alpha_2[1 + \mu_n q_n(\alpha_2)], \text{ mod. } P^{n+1},$$

we should have

$$\alpha_1 - \alpha_2 \equiv \mu_n[\alpha_2 q_n(\alpha_2) - \alpha_1\mu_n q_n(\alpha_1)], \text{ mod. } P^{n+1},$$

which is impossible, since $\alpha_1 - \alpha_2$ is not divisible by P^n.

Now by giving to n the values $1, 2, 3, \cdots$ we thus see that all the roots of

$$x^{\phi(P)} \equiv 1, \text{ mod. } P^n,$$

are

$$(10) \quad x \equiv \alpha[1 + \mu_1 q_1(\alpha)] \cdots [1 + \mu_{n-1} q_{n-1}(\alpha)], \text{ mod. } P^n,$$

where α runs through the roots of

$$x^{\phi(P)} \equiv 1, \text{ mod. } P.$$

PURDUE UNIVERSITY,
August, 1903.

MACH'S MECHANICS.

The Science of Mechanics — a Critical and Historical Account of its Development. By ERNST MACH. Translated from the German by T. J. MCCORMACK. Second revised and enlarged edition. Chicago, The Open Court Publishing Co., 1902. xix + 605 pp.

IN a recent review of the German edition of Routh's Rigid Dynamics, BULLETIN, May, 1902, we expressed the desire